Remarks

In the official action, the Examiner made an objection to claim 52, noting that it has a minor error in dependency. As the Examiner will note by reference to the claim amendments made, claim 52 has been corrected. The Examiner is thanked for pointing this matter out.

The Examiner rejected claims 1-10, 12-17 and 22-52 as allegedly being fully anticipated by US Patent No. 5,892,900 to Ginter. This grounds for rejection is respectfully traversed. The Examiner directs the Applicant's attention to column 68, lines 29-42 of Ginter. At this portion of Ginter, there is discussion of an optional pattern matching engine 524 which is shown, incidentally, in Figure 9 of Ginter. If the pattern matching engine 524 of Ginter is supposed to anticipate the trusted device of claim 1, it is not understood how it is "arranged to acquire a true value of an integrity metric of the computing apparatus" as specifically claimed by claim 1. While it is true that the discussion in Ginter at the point mentioned by the Examiner the word "metrics" is used, but it is in the context of searching potentially long strings of data for certain bit patterns or other significant pattern related metrics. It is not understood what this has to do with the subject matter being claimed.

The Examiner is invited to go back and read the background and summary of the Ginter et al. patent. At those points in the disclosure, Ginter tells us that his invention provides a new kind of "virtual distribution environment" (VDE) that secures and administers and audits electronic information use. The reader is told that VDE features fundamentally important capabilities for managing content that travels across the information highway. These capabilities, the reader is told, comprise a rights protection solution that serves all electronic community members.

Ginter is also concerned with providing a secure processing environment that has a tamper resistant barrier. See Figure 6, for example.

However, what happens if the tamper resistant barrier is breached by someone who has the desire and ability to do so? Does the Ginter system recognize that a breach has occurred so as to be able to provide a different "true value of an integrity metric of the computing apparatus" than would be provided if no breach had occurred? Ginter certainly does not teach that at the point referred to by the Examiner in column 68.

It is submitted that the rejection of claim 1 based on Ginter is improper and therefore this grounds for rejection should be withdrawn.

Turning to claims 2-10 and 44-49, the Examiner asserts that these claims teach a "similar" apparatus of claim 1 and therefore are rejected in a "similar" manner. While these claims are dependent upon claim 1, that does not mean that they do not have limitations that the Examiner can just ignore. For example, claim 3

recites, among other things, that the trusted device is "arranged to transfer the instructions of the program code to the main processing means." Where does Ginter show that? Claim 4 indicates that the computing apparatus is arranged to cause the instructions from the trusted device "to be the first instructions executed after release from reset." Where does Ginter even hint at such a feature?

Claim 6 recites that the trusted device "is arranged to monitor a data bus means by which components mounted on the assembly are adapted to communicate and store in the memory means a flag in the event that the first memory read signal is generated by the main processing means after the computing system is released from reset or addressed to the trusted device." Where is this feature shown by Ginter?

The Examiner is respectfully reminded that it is the Examiner's obligation to point the Applicant to where the material is allegedly disclosed when rejecting claims. Please see 37 CFR 1.04(2)(c ) wherein the Rules of Practice indicate that when "a reference is complex or shows or describes inventions other than that claimed by the Applicant, the particular part relied upon must be designated as clearly as practicable" by the Examiner. Ginter is certainly a complex reference, given the fact that it is over 300 pages long! The Rule also requires that the pertinence of each reference, if not apparent, "must be clearly explained and each rejected claim specified."

It is not up to the Applicant to have to speculate as to why the Examiner is rejecting the claims in this application. However, as things presently stand, the Applicant has not the faintest notion why a claim, such as claims 3, 4 and 6, for example, is being rejected by the Examiner. Since the Examiner made the rejection under 35 U.S.C. 102, that means that the prior art reference is supposed to teach each and every limitation of these claims. How can it possibly be that column 68, lines 29-42 teach each and every limitation of any of the rejected claims in this application?

Turning now to claim 12, the Examiner also asserts that that claim is fully anticipated by Ginter. This grounds for rejection is respectfully traversed.

Claim 12 is a method claim that starts off by reciting that the trusted device acquires "the true value of the integrity metric of the trusted computing apparatus." The Examiner asserts that box 524 in Figure 9 meets that limitation. Box 524 reflects nothing more than the pattern matching machine discussed at column 68, lines 29-42. As discussed above, although that section of Ginter does use the word "metrics", it is asserted that the section to which the Examiner points is utterly silent with respect to "the integrity metric of the trusted computing apparatus" specifically mentioned in claim 12.

Claim 12 also recites "the user generating a challenge for the trusted computing apparatus to prove its integrity and submitting the challenge to the trusted computing apparatus." The Examiner again cites column 68, lines 29-42 of Ginter. Where is there a hint or suggestion of generating a challenge and submitting a challenge in the lines noted by the Examiner? The lines cited by the

Examiner do speak, briefly, about validation/authentication of VDE objects and other items, but how does that relate to "generating a challenge for the trusted computer apparatus to prove its integrity" or "submitting the challenge to the trusted computing apparatus" as specifically claimed by claim 12?

Turning now to a limitation of claim 12 that recites that the "trusted computing apparatus receiving the challenge and the trusted device generating a response including the integrity metric and returning the response to the user". The Examiner points the Applicant to column 19, lines 29-58 of Ginter.

Before addressing the specific language cited by the Examiner, it is also helpful to read the context in which the disclosure at column 19 occurs. See, for example, the disclosure that begins at column 17, line 18, wherein Ginter provides some background information with respect to his VDEs. Note that the VDE electronic transaction management mechanisms can "enforce the electronic rights and agreements of all parties participating in widely varying business and data security models and that this could be efficiently achieved through a single VDE implementation within each VDE participants electronic appliance.

Of course, it is important over the Internet to have mechanisms which can enforce electronic rights and agreements of parties doing business on the Internet and at column 19, lines 29-58 the VDE electronic agreement is discussed further in that the parties, apparently, can evaluate the agreements as to whether "certain other electronic terms and conditions attached to content and/or submitted by another party are acceptable." Of course, such an evaluation process might well be important in the context of doing business over the Internet.

However, what does that have to do with the limitation quoted above from claim 12 that recites that the trusted computing apparatus receives the challenge and "the trusted device generating a response including the integrity metric and returning the response to the user"? Note that the integrity metric is the integrity metric mentioned in the preamble of the claim, namely the integrity metric of the trusted computing apparatus.

Although Ginter is concerned with transferring data in a secure fashion between users and making sure that VDE participants have ways of reviewing agreements to ensure that they are acceptable to the parties, where does Ginter have anything whatsoever to do with the integrity metric of the trusted computing apparatus? In reviewing the portions of Ginter cited by the Examiner, Ginter appears to be almost silent when it comes to the security of a computer apparatus other than the fact that Ginter seems to suggest that the physical security may be important noting the reference to a tamper resistant barrier in Figure 6 of Ginter.

Moving on, claim 12 also recites "the user receiving the response, extracting the integrity metric from the response and comparing the integrity metric with an authenticated metric for the trusted computing apparatus that has been

generated by a trusted party." With respect to this element of claim 12, the Examiner refers the Applicant to column 9, lines 19-30.

It is a bit of a mystery what the Ginter disclosure is supposed to be teaching at this point. For example, the discussion there could be nothing more than a highly generalized discussion of a web browser using SSL security to visit an encrypted web site where a person would do their banking and perhaps even make payments to vendors. The description of Ginter at that point is seemingly broad enough to cover such activities. However, what does that have to do with "comparing the integrity metric of the trusted computing apparatus with an authenticated metric for the trusted computing apparatus" as specifically claimed by claim 12?

Since Ginter, at least in the portion cited by the Examiner, appears to be not at all concerned with the integrity metric of a trusted computing apparatus, Ginter appears to be utterly irrelevant to claim 12. Why is the Examiner even bothering to cite Ginter?

Turning to claim 13, claim 13 recites that the challenge includes a nonce and that the response includes the integrity metric and the nonce, both digitally signed by the trusted device using an information security algorithm. The Examiner takes the position that claim 13 is anticipated merely because Ginter allegedly teaches a method with a security algorithm, pointing to column 45, lines 49-62 of Ginter.

With all due respect to the Examiner, at this point in Ginter, there is a discussion that indicates that the degree of trustedness of a VDE arrangement are based upon a number of things which starts off with the question of whether or not hardware SPUs are employed. However, none of this has anything to do with the integrity metric of the machine. Ginter seems to point the reader to either use a hardware SPUs or to relying on physical facility security and user identity authentication procedures if hardware SPUs cannot be used. Ginter is pointing to old-fashioned techniques of either locking the hardware up so that it cannot be easily breached or restricting those people who have physical access to the hardware. The invention of claim 13 is fundamentally different since it is concerned with the integrity metric defined in claim 12, that is, the integrity metric of the computing apparatus.

It is not understood how the disclosure at column 45, lines 49-62 has anything to whatsoever to do with claim 13 of the present application. Additionally, it should be noted that claim 13 recites that the challenge includes a nonce. Where is there any discussion of a nonce in Ginter?

With respect to claims 14-17 and 50, the Examiner asserts that these claims teach a "similar" method of claim 12 and therefore are rejected in a "similar" manner. With all due respect to the Examiner, this is not a proper rejection. The Rules of Practice, as indicated above, require that the Examiner specifically point out for each limitation of each claim exactly where the limitation is taught or suggested by the prior art. These rejections are procedurally improper.

Not only are these rejections procedurally improper, they are without merit. For example, claim 14 recites that the trusted device uses "a private encryption key to sign the integrity metric and the nonce and the user uses the respective public encryption key to verify the integrity metric and the nonce." Since Ginter appears to be silent with respect to the use or non-use of a nonce or the use of an integrity metric, how can the Examiner possibly take the position that claim 14 is fully anticipated by Ginter?

Turning to claim 15, where is there any disclosure in Ginter that the user "uses the public encryption key from the certificate to verify the integrity metric in the nonce" as specifically cited by claim 15? How is that met by Ginter, given the fact that Ginter is silent with respect to both integrity metrics and nonces?

Of course, the Applicant can go through each one of the dependent claims and ask the Examiner exactly how those claims are anticipated by the prior art. Indeed, if the Examiner continues to reject any of the claims in this application on prior art grounds, the Examiner is respectfully requested to comply with the Rules of Practice, particularly 37 CFR 1.104, in the manner in which the Examiner cites prior art against the claims.

Finally, turning to claim 22, claim 22 recites, inter alia, that "the trusted device is adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric." In rejecting this claim, the Examiner again takes us back to Figure 9 and column 68, lines 29-42. However, as previously mentioned, Ginter appears to be absolutely silent on the matter of an integrity metric which, in the case of claim 22, "measures that the computing apparatus is operating as intended." Ginter, in the portion cited by the Examiner, appears to assume that the computing apparatus is operating as intended and therefore is doing its encryptions and comparisons, and whatever. However, as disclosed in the present application, that is a bad assumption to make, because someone with physical access to the computer could open it up and install, for example, a rogue BIOS chip, allowing the third party to access the computer unbeknownst to its usual user. As previously indicated, Ginter apparently relies upon physical security or upon the trustworthiness of individuals who have physical access to the computer systems disclosed in Ginter for their protection. Ginter, in the portions pointed out by the Examiner in the official action, appears to take no heed as to whether a computer system has been successfully and surreptitiously violated and therefore apparently is not concerned whatsoever with respect to acquiring "a value of an integrity metric that measures that the computing apparatus is operating as intended" as specifically claimed by claim 22. As such, the Applicant is at a complete loss to understand why the Examiner is even bothering to cite Ginter against claim 22.

The Examiner rejects claims 23-43, 51 and 52 asserting that each of these claims teach a "similar" apparatus of claim 12 and is therefore rejected in a "similar" manner. As indicated above, this rejection violates the Rules of Practice in that the Examiner has the obligation of pointing out where each and every limitation of each and every claim is allegedly met by the prior art. It is not up to the

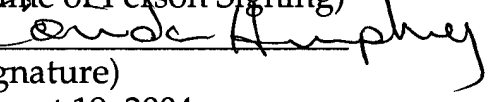
Applicant to have to make a fishing expedition through the Ginter reference to try to figure out what the Examiner may have had in mind when rejecting each one of these claims. And, if the Examiner had no reasons for rejecting those claims based upon the disclosure of Ginter, then such rejections are also improper.

In summary, the rejections based on Ginter are utterly without merit. If the Examiner is not prepared to allow this application or at least cite art that is relevant to its claims, then the Examiner is respectfully requested to issue a final rejection so that the Applicant can pursue this matter with the Board of Appeals.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 12-0415. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 12-0415.

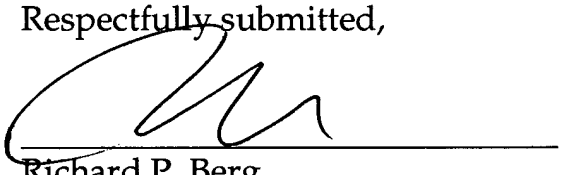
I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents
POB 1450, Alexandria, VA 22313-1450 on

August 19, 2004
(Date of Deposit)
Corinda Humphrey
(Name of Person Signing)



(Signature)
August 19, 2004
(Date)

Respectfully submitted,



Richard P. Berg
Attorney for Applicants
Reg. No.28,145
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300